PCT/JP2004/016708

日本国特許庁
JAPAN PATENT OFFICE

04.11.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月１０日

出願番号
Application Number: 特願２００４－０３４１７２
[ST. 10/C]: [ＪＰ２００４－０３４１７２]

出願人
Applicant(s): エヌ・ティ・ティ・コミュニケーションズ株式会社

２００４年１２月１３日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１１３６５７

【書類名】　特許願
【整理番号】　GLN00468
【提出日】　平成16年 2月10日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 17/00
　　H04L 12/22

【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　深田　聡
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　山崎　俊之
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　白崎　泰弘
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　齊藤　允
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　徳永　治
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　内山　貴允
【特許出願人】
　【識別番号】　399035766
　【氏名又は名称】　エヌ・ティ・ティ・コミュニケーションズ株式会社
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2003-374880
　【出願日】　平成15年11月 4日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0113902

【書類名】特許請求の範囲
【請求項１】
ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するための方法であって、
前記ネットワークに接続されたセッション管理装置と第１の端末との間で相互認証を行い、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立するステップと、
セッション管理装置と第２の端末との間で相互認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立するステップと、
第１の暗号化通信チャネルと第２の暗号化通信チャネルとを介して第１の端末と第２の端末との間で鍵情報を交換するステップと
を有することを特徴とする方法。
【請求項２】
ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するための方法であって、
前記ネットワークに接続されたセッション管理装置と第１の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第１の端末が相互に認証を行い、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立するステップと、
セッション管理装置と第２の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第２の端末が相互に認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立するステップと、
第１の端末が、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む第２の端末への接続要求メッセージを第１の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その接続要求メッセージを第２の暗号化通信チャネルを介して第２の端末に送信するステップと、
第２の端末が、前記接続要求メッセージへの応答として、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第２の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その応答メッセージを第１の暗号化通信チャネルを介して第１の端末に送信するステップと
を有することを特徴とする方法。
【請求項３】
第１の端末とセッション管理装置との間のメッセージ通信、及び第２の端末とセッション管理装置との間のメッセージ通信をＳＩＰに基づき行う請求項１又は２に記載の方法。
【請求項４】
第１の端末が、前記第１の暗号化通信チャネルを介して、第１の端末の名前とアドレスをセッション管理装置に登録するステップと、
第２の端末が、前記第２の暗号化通信チャネルを介して、第２の端末の名前とアドレスをセッション管理装置に登録するステップとを更に有し、
第１の端末から送信される前記接続要求メッセージは第２の端末の名前を含み、前記セッション管理装置は、当該名前から第２の端末のアドレスを取得し、当該アドレス宛に前記接続要求メッセージを送信する請求項２に記載の方法。
【請求項５】
前記セッション管理装置は、端末間で接続を許可するか否かの情報を保持し、接続要求メッセージを受信した場合に、当該情報を参照して、接続要求元の端末が接続要求先の端末と接続することが許容されているか否かを判断し、許容されていない場合には、接続を拒否する請求項２に記載の方法。
【請求項６】
前記第１の端末が第３の端末からのアクセスを受けた後に前記各ステップが実行され、前記各ステップの実行により確立された前記第１の端末と前記第２の端末との間の暗号化通信チャネルを介して、前記第１の端末が前記第２の端末からデータを受信し、当該デー

タを前記第３の端末に送信する請求項１又は２に記載の方法。
【請求項７】
前記第１の端末が第３の端末からのアクセスを受けた後に、前記第１の暗号化通信チャネル及び前記第２の暗号化通信チャネル確立のためのステップ以降の各ステップが実行され、当該各ステップの実行により確立された前記第１の端末と前記第２の端末との間の暗号化通信チャネルを介して、前記第１の端末が前記第２の端末からデータを受信し、当該データを前記第３の端末に送信する請求項１又は２に記載の方法。
【請求項８】
ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するための方法であって、
前記ネットワークに接続された公開鍵管理装置と第１の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第１の端末が相互に認証を行う暗号化通信チャネル確立ステップと、
第１の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第１の端末との間の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、
公開鍵管理装置が、受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第１の端末との間の前記暗号化通信チャネルを介して第１の端末に送信するステップと、
第１の端末が、第２の端末に当該公開鍵証明書を配布することにより、第１の端末と第２の端末との間で公開鍵を用いた暗号化通信チャネルを確立するステップと
を有することを特徴とする方法。
【請求項９】
前記公開鍵管理装置は、前記暗号化通信チャネル確立ステップを実行して第１の端末との間で前記暗号化通信チャネルを確立するサーバと、当該サーバに暗号化通信チャネルを介して接続された公開鍵証明書を生成・管理する機能を有する装置とからなる請求項８に記載の方法。
【請求項１０】
第１の端末と公開鍵管理装置との間のメッセージ通信をＳＩＰに基づき行う請求項８又は９に記載の方法。
【請求項１１】
ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するための方法であって、
前記ネットワークに接続された公開鍵管理装置と第１の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第１の端末が相互に認証を行う第１の暗号化通信チャネル確立ステップと、
公開鍵管理装置と第２の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第２の端末が相互に認証を行う第２の暗号化通信チャネル確立ステップと、
第１の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記第１の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第１の端末との間の第１の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、
公開鍵管理装置は受信した公開鍵を記憶装置に格納し、第２の端末が、当該公開鍵を、前記第２の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第２の端末との間の第２の暗号化通信チャネルを介して取得するステップと、
第１の端末と第２の端末との間で当該公開鍵を用いた暗号化通信チャネルを確立するステップと
を有することを特徴とする方法。
【請求項１２】
前記公開鍵管理装置は、第１の端末との間、及び第２の端末との間で暗号化通信チャネルを確立する装置と、当該装置と暗号化通信チャネルを介して接続された公開鍵を管理す

る機能を有する装置とからなる請求項１１に記載の方法。
【請求項１３】
第１の端末と公開鍵管理装置との間のメッセージ通信、及び第２の端末と公開鍵管理装置との間のメッセージ通信をＳＩＰに基づき行う請求項１１又は１２に記載の方法。
【請求項１４】
ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するためのセッション管理装置であって、
第１の端末との間で暗号化通信のための鍵情報を交換し、第１の端末と相互に認証を行い、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立する手段と、
第２の端末との間で暗号化通信のための鍵情報を交換し、第２の端末と相互に認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立する手段と、
第１の端末から、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む第２の端末への接続要求メッセージを第１の暗号化通信チャネルを介して受信し、その接続要求メッセージを第２の暗号化通信チャネルを介して第２の端末に送信する手段と、
第２の端末から、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第２の暗号化通信チャネルを介して受信し、その応答メッセージを第１の暗号化通信チャネルを介して第１の端末に送信する手段と
を有することを特徴とするセッション管理装置。
【請求項１５】
第１の端末とセッション管理装置との間のメッセージ通信、及び第２の端末とセッション管理装置との間のメッセージ通信をＳＩＰに基づき行う手段を有する請求項１４に記載のセッション管理装置。
【請求項１６】
前記第１の暗号化通信チャネルを介して第１の端末の名前とアドレスを受信し、記憶装置に登録する手段と、
前記第２の暗号化通信チャネルを介して第２の端末の名前とアドレスを受信し、記憶装置に登録する手段とを更に有し、
第１の端末から送信される前記接続要求メッセージは、第２の端末の名前を含み、前記セッション管理装置は、当該名前から第２の端末のアドレスを取得する名前解決手段を有する請求項１４に記載のセッション管理装置。
【請求項１７】
前記セッション管理装置は、端末間で接続を許可するか否かの情報を保持し、接続要求メッセージを受信した場合に、当該情報を参照して、接続要求元の端末が接続要求先の端末と接続することが許容されているか否かを判断し、許容されていない場合には、接続を拒否する手段を有する請求項１４に記載のセッション管理装置。
【請求項１８】
ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置であって、
第１の端末との間で暗号化通信のための鍵情報を交換し、第１の端末と相互に認証を行う暗号化通信チャネル確立手段と、
第１の端末から、前記暗号化通信チャネル確立手段により確立された公開鍵管理装置と第１の端末との間の暗号化通信チャネルを介して、第１の端末の公開鍵を受信する手段と、
受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第１の端末との間の前記暗号化通信チャネルを介して第１の端末に送信する手段と
を有することを特徴とする公開鍵管理装置。
【請求項１９】
前記公開鍵管理装置は、前記暗号化通信チャネル確立手段を有するサーバと、当該サー

バに暗号化通信チャネルを介して接続された公開鍵証明書を生成・管理する機能を有する装置とからなる請求項１８に記載の公開鍵管理装置。
【請求項２０】
第１の端末と公開鍵管理装置との間のメッセージ通信をＳＩＰに基づき行う手段を有する請求項１８又は１９に記載の公開鍵管理装置。
【請求項２１】
ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置であって、
第１の端末との間で暗号化通信のための鍵情報を交換し、第１の端末と相互に認証を行う第１の暗号化通信チャネル確立手段と、
第２の端末との間で暗号化通信のための鍵情報を交換し、第２の端末と相互に認証を行う第２の暗号化通信チャネル確立手段と、
第１の端末から、前記第１の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第１の端末との間の第１の暗号化通信チャネルを介して、第１の端末の公開鍵を受信する手段と、
受信した公開鍵を記憶装置に格納する手段と、
前記第２の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第２の端末との間の第２の暗号化通信チャネルを介して、第１の端末の公開鍵を第２の端末に送信する手段と
を有することを特徴とする公開鍵管理装置。
【請求項２２】
前記公開鍵管理装置は、第１の端末との間、及び第２の端末との間で暗号化通信チャネルを確立する装置と、当該装置に暗号化通信チャネルを介して接続された公開鍵を管理する機能を有する装置とからなる請求項２１に記載の公開鍵管理装置。
【請求項２３】
第１の端末と公開鍵管理装置との間のメッセージ通信、及び第２の端末と公開鍵管理装置との間のメッセージ通信をＳＩＰに基づき行う手段を有する請求項２１又は２２に記載の公開鍵管理装置。
【請求項２４】
ネットワークに接続されたセッション管理装置を用いて第２の端末との間で暗号化通信チャネルを確立する端末であって、
ネットワークに接続されたセッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化通信チャネルを確立する第１の暗号化通信チャネル確立手段と、
前記端末と前記第２の端末との間の暗号化通信のための鍵情報を含む前記第２の端末への接続要求メッセージを、前記暗号化通信チャネル確立手段により確立された暗号化通信チャネルを介してセッション管理装置に送信し、前記第２の端末から、セッション管理装置を介して、前記端末と前記第２の端末との間の暗号化通信のための鍵情報を含む応答メッセージを受信することにより、前記第２の端末との間で暗号化通信チャネルを確立する第２の暗号化通信チャネル確立手段と
を有することを特徴とする端末。
【請求項２５】
前記端末は、第３の端末からのアクセスを受けた後に、前記端末と前記セッション管理装置との間の暗号化通信チャネルを確立するための処理と、前記端末と前記第２の端末との間の暗号化通信チャネルを確立するための処理を実行し、
前記端末と前記第２の端末との間の暗号化通信チャネルを介して前記第２の端末からデータを受信し、そのデータを前記第３の端末に送信する請求項２４に記載の端末。
【請求項２６】
前記端末は、第３の端末からのアクセスを受けた後に、前記端末と前記第２の端末との間の暗号化通信チャネルを確立するための処理を実行し、

前記端末と前記第２の端末との間の暗号化通信チャネルを介して前記第２の端末からデータを受信し、そのデータを前記第３の端末に送信する請求項２４に記載の端末。
【請求項２７】
前記端末は、前記第３の端末に対して許容されている少なくとも１つの接続先を示すテーブルを備え、前記第３の端末からのアクセスに応じて当該少なくとも１つの接続先の情報を前記第３の端末に送信し、前記第３の端末から接続先の指定を受ける請求項２５又は２６に記載の端末。
【請求項２８】
コンピュータを、ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するためのセッション管理装置として機能させるプログラムであって、コンピュータを、
第１の端末との間で暗号化通信のための鍵情報を交換し、第１の端末と相互に認証を行い、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立する手段、
第２の端末との間で暗号化通信のための鍵情報を交換し、第２の端末と相互に認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立する手段、
第１の端末から、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む第２の端末への接続要求メッセージを第１の暗号化通信チャネルを介して受信し、その接続要求メッセージを第２の暗号化通信チャネルを介して第２の端末に送信する手段、
第２の端末から、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第２の暗号化通信チャネルを介して受信し、その応答メッセージを第１の暗号化通信チャネルを介して第１の端末に送信する手段
として機能させるプログラム。
【請求項２９】
コンピュータを、ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置として機能させるプログラムであって、コンピュータを、
第１の端末との間で暗号化通信のための鍵情報を交換し、第１の端末と相互に認証を行う暗号化通信チャネル確立手段、
第１の端末から、前記暗号化通信チャネル確立手段により確立された公開鍵管理装置と第１の端末との間の暗号化通信チャネルを介して、第１の端末の公開鍵を受信する手段、
受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第１の端末との間の前記暗号化通信チャネルを介して第１の端末に送信する手段
として機能させるプログラム。
【請求項３０】
コンピュータを、ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置として機能させるプログラムであって、コンピュータを、
第１の端末との間で暗号化通信のための鍵情報を交換し、第１の端末と相互に認証を行う第１の暗号化通信チャネル確立手段、
第２の端末との間で暗号化通信のための鍵情報を交換し、第２の端末と相互に認証を行う第２の暗号化通信チャネル確立手段、
第１の端末から、前記第１の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第１の端末との間の第１の暗号化通信チャネルを介して、第１の端末の公開鍵を受信する手段、
受信した公開鍵を記憶装置に格納する手段、
前記第２の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第２の端末との間の第２の暗号化通信チャネルを介して、第１の端末の公開鍵を第２の端末に送信する手段

として機能させるプログラム。
【請求項３１】
コンピュータを、ネットワークに接続されたセッション管理装置を用いて他の端末との間で暗号化通信チャネルを確立する端末として機能させるプログラムであって、コンピュータを、
ネットワークに接続されたセッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化通信チャネルを確立する暗号化通信チャネル確立手段、
前記端末と前記他の端末との間の暗号化通信のための鍵情報を含む前記他の端末への接続要求メッセージを、前記暗号化通信チャネル確立手段により確立された暗号化通信チャネルを介してセッション管理装置に送信し、前記他の端末から、セッション管理装置を介して、前記端末と前記他の端末との間の暗号化通信のための鍵情報を含む応答メッセージを受信する手段
として機能させるプログラム。

【書類名】明細書
【発明の名称】端末間の暗号化通信チャネルを構築する方法及びそのための装置並びにプログラム
【技術分野】
【０００１】
本発明は、ネットワーク上の２つの端末間でセキュアなデータチャネルを構築する技術に関するものである。
【背景技術】
【０００２】
従来技術において、ＩＰネットワーク上の２つの端末間でデータチャネルを構築しいわゆるピア・ツー・ピアの通信を行うためには、ＤＮＳへの名前登録から、セキュリティを確保するためのＦＷ等の設定・管理、証明書の取得等の作業が必要である。また、多数の端末同士の間で相互認証および暗号化されたピア・ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のＩＤ、パスワードを管理することが必要である。
【０００３】
このように、従来技術では、ＩＰネットワーク上の２つの端末間でセキュアなデータチャネルを構築するために煩雑な作業が必要である上、オープンなＤＮＳに名前とアドレスが登録されるため、端末が不正なアクセスを受ける恐れがあるという問題がある。
【０００４】
また、端末間に仲介サーバを導入し、一方の端末からのデータチャネルを代理で終端し、他方の端末のデータチャネルも代理で終端し、両端末のデータチャネルを仲介サーバ上でマッチングさせることにより、擬似的に２つの端末間のデータチャネルを実現するしくみも提案されている。しかしながら、この方法には、端末同士の全てのデータが仲介サーバを経由するため、仲介サーバに多大な負荷がかかるという問題がある。また、家庭内端末に対するリアルタイムなアクセスができないという問題もある。
【特許文献１】特開２００２－２０８９２１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
本発明は、上記の点に鑑みてなされたものであり、端末間でセキュアなデータチャネルを容易に構築するための技術を提供することを目的とする。
【課題を解決するための手段】
【０００６】
上記の課題は、ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するための方法であって、前記ネットワークに接続されたセッション管理装置と第１の端末との間で相互認証を行い、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立するステップと、セッション管理装置と第２の端末との間で相互認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立するステップと、第１の暗号化通信チャネルと第２の暗号化通信チャネルとを介して第１の端末と第２の端末との間で鍵情報を交換するステップとを有する方法により解決できる。
【０００７】
本発明によれば、相互認証を行うことにより各端末とセッション管理装置との間で相互信頼の関係が築け、これにより、第１の端末と第２の端末との間では、セッション管理装置を介した簡易なシグナリング手順により、暗号化通信チャネルを確立でき、端末間でセキュアなデータチャネルを容易に構築できる。また、その後の端末間通信はセッション管理装置を介することなく行うことができるので、従来の問題が解決される。
【０００８】
また、上記の課題は、ネットワークに接続された第１の端末と第２の端末との間で暗号

化通信チャネルを確立するための方法であって、前記ネットワークに接続されたセッション管理装置と第１の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立するステップと、セッション管理装置と第１の端末が相互に認証を行い、セッション管理装置と第２の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第２の端末が相互に認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立するステップと、第１の端末が、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む第２の端末への接続要求メッセージを第１の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その接続要求メッセージを第２の暗号化通信チャネルを介して第２の端末に送信するステップと、第２の端末が、前記接続要求メッセージへの応答として、第１の端末と第２の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第２の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その応答メッセージを第１の暗号化通信チャネルを介して第１の端末に送信するステップとを有する方法によっても解決できる。

【０００９】

上記の方法において、第１の端末とセッション管理装置との間のメッセージ通信、及び第２の端末とセッション管理装置との間のメッセージ通信をＳＩＰに基づき行うことができる。

【００１０】

また、第１の端末が、前記第１の暗号化通信チャネルを介して、第１の端末の名前とアドレスをセッション管理装置に登録するステップと、第２の端末が、前記第２の暗号化通信チャネルを介して、第２の端末の名前とアドレスをセッション管理装置に登録するステップとを更に有し、第１の端末から送信される前記接続要求メッセージは第２の端末の名前を含み、前記セッション管理装置は、当該名前から第２の端末のアドレスを取得し、当該アドレス宛に前記接続要求メッセージを送信するようにしてもよい。

【００１１】

更に、前記セッション管理装置は、端末間で接続を許可するか否かの情報を保持し、接続要求メッセージを受信した場合に、当該情報を参照して、接続要求元の端末が接続要求先の端末と接続することが許容されているか否かを判断し、許容されていない場合には、接続を拒否することができる。

【００１２】

また、前記第１の端末が第３の端末からのアクセスを受けた後に前記各ステップが実行され、前記各ステップの実行により確立された前記第１の端末と前記第２の端末との間の暗号化通信チャネルを介して、前記第１の端末が前記第２の端末からデータを受信し、当該データを前記第３の端末に送信するようにしてもよい。

【００１３】

更に、前記第１の端末が第３の端末からのアクセスを受けた後に、前記第１の暗号化通信チャネル及び前記第２の暗号化通信チャネル確立のためのステップ以降の各ステップが実行され、前記各ステップの実行により確立された前記第１の端末と前記第２の端末との間の暗号化通信チャネルを介して、前記第１の端末が前記第２の端末からデータを受信し、当該データを前記第３の端末に送信するようにしてもよい。

【００１４】

また、上記の課題は、ネットワークに接続された第１の端末と第２の端末との間に暗号化通信チャネルを確立するための方法であって、前記ネットワークに接続された公開鍵管理装置と第１の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第１の端末が相互に認証を行う暗号化通信チャネル確立ステップと、第１の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第１の端末との間の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、公開鍵管理装置が、受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第１の端末との間の前記暗号化通信チャネルを介して第１の

端末に送信するステップと、第１の端末が、第２の端末に当該公開鍵証明書を配布することにより、第１の端末と第２の端末との間で公開鍵を用いた暗号化通信チャネルを確立するステップとを有する方法によっても解決できる。

【００１５】

本発明によれば、従来のように煩雑な手続きを得ることなく、公開鍵ベースの暗号化通信チャネルを確立できる。

【００１６】

なお、前記公開鍵管理装置は、前記暗号化通信チャネル確立ステップを実行して第１の端末との間で前記暗号化通信チャネルを確立するサーバと、当該サーバに暗号化通信チャネルを介して接続された公開鍵証明書を生成・管理する機能を有する装置とからなるように構成してもよい。

【００１７】

また、第１の端末と公開鍵管理装置との間のメッセージ通信はＳＩＰに基づき行うことができる。

【００１８】

また、上記の課題は、ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するための方法であって、前記ネットワークに接続された公開鍵管理装置と第１の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第１の端末が相互に認証を行う第１の暗号化通信チャネル確立ステップと、公開鍵管理装置と第２の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第２の端末が相互に認証を行う第２の暗号化通信チャネル確立ステップと、第１の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記第１の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第１の端末との間の第１の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、公開鍵管理装置は受信した公開鍵を記憶装置に格納し、第２の端末が、当該公開鍵を、前記第２の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第２の端末との間の第２の暗号化通信チャネルを介して取得するステップと、第１の端末と第２の端末との間で当該公開鍵を用いた暗号化通信チャネルを確立するステップとを有する方法によっても解決できる。

【００１９】

前記公開鍵管理装置は、第１の端末との間、及び第２の端末との間で暗号化通信チャネルを確立する装置と、当該装置と暗号化通信チャネルを介して接続された公開鍵を管理する機能を有する装置とからなるように構成してもよく、第１の端末と公開鍵管理装置との間のメッセージ通信、及び第２の端末と公開鍵管理装置との間のメッセージ通信をＳＩＰに基づき行うこともできる。

【００２０】

また、本発明によれば、上記の方法における処理を行うセッション管理装置、端末、及びプログラムが提供される。

【発明の効果】

【００２１】

本発明によれば、端末間でセキュアなデータチャネルを容易に構築できる。また、その後の端末間通信はセッション管理装置を介することなく行うことができるので、仲介サーバを用いる場合の従来の問題が解決される。

【発明を実施するための最良の形態】

【００２２】

以下、本発明の実施の形態を図を参照して説明する。

【００２３】

（第１の実施の形態）

まず、図１を用いて本発明の第１の実施の形態の概要について説明する。

【００２４】

図１に示すように、端末１と端末２との間にセッション管理サーバ３を設置し、端末１

－セッション管理サーバ３－端末２間で、端末１－端末２間のデータチャネル構築のためのシグナリング（信号手順）を実行し、データチャネル構築後はセッション管理サーバ３を介さずに端末間のみでデータ通信を行うというものである。

【００２５】

シグナリングにおいては、まず、端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間の各々で、ＩＰｓｅｃ等の暗号化通信を行うためのセキュアシグナリングチャネル確立のために、暗号鍵情報の交換、相互認証が行われる。そして、端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間の各々で確立されたセキュアシグナリングチャネルを介してセッション管理サーバへの名前登録、端末１－端末２間のセキュアデータチャネル確立のためのシグナリングが実行される。

【００２６】

端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間でのセキュアシグナリングチャネル確立におけるシグナリングにより、セッション管理サーバ３と端末１との間、セッション管理サーバ３と端末２との間において相互認証に基づく信頼関係が確立されているため、端末１と端末２との間でも信頼関係が確立されている。すなわち、上記の相互認証により、セッション管理サーバ３を介した信頼のチェーンモデルが構築される。従って、端末１－端末２間のセキュアデータチャネル確立のためのシグナリングでは、簡易な鍵情報の交換手順を用いることができる。

【００２７】

次に、端末１－セッション管理サーバ３－端末２間の通信のシーケンスを図２を参照して説明する。

【００２８】

図２に示すシーケンスは、端末１、セッション管理サーバ３、端末２がインターネット等のＩＰネットワークに接続されたシステム構成を前提とするものである。

【００２９】

各端末は、セッション管理サーバ３との間でシグナリングを実行するシグナリング機能、セキュアデータチャネルを介してデータ通信を行うための機能、及びデータ通信を利用して所望のサービスを提供するアプリケーションを備えている。

【００３０】

また、セッション管理サーバは、シグナリングを各端末との間で実行するシグナリング機能、端末間の接続許可等を制御する接続ポリシー制御機能、各端末を認証するための認証機能、端末の名前からＩＰアドレスを取得する名前解決機能、及び、認証のために用いるＩＤ、パスワードを格納するデータベースや、名前とＩＰアドレスを対応付けて格納するデータベース等を備えている。また、名前解決機能として一般のＤＮＳと同等の機能を持たせることもできる。

【００３１】

図２に示すように、端末１－端末２間でのセキュアデータチャネル構築にあたり、まず、端末１－セッション管理サーバ３間、端末２－セッション管理サーバ３間の各々でセキュアシグナリングチャネルを構築して、名前の登録を行う。

【００３２】

すなわち、端末１－セッション管理サーバ３間でＩＰｓｅｃ等の暗号通信で用いる鍵情報（暗号鍵生成用の情報）の交換を行う（ステップ１）。その後、自分のＩＤ、パスワードを含む情報を暗号化して相手側に送信することにより、相互に認証を行う（ステップ２）。認証後は、セキュアシグナリングチャネルが確立された状態となり、そのチャネルを用いて、端末１は名前とＩＰアドレスの登録をセッション管理サーバ３に対して行う（ステップ３）。端末１の通信相手となる端末２とセッション管理サーバ３間でも同様のシーケンスが実行され、端末２の名前とＩＰアドレスがセッション管理サーバ３に登録される（ステップ４、５、６）。

【００３３】

その後、端末１から端末２への接続要求が、セキュアシグナリングチャネルを介して送

信される（ステップ７）。接続要求には、端末２の名前と暗号通信用の鍵情報（暗号鍵生成用の情報）が含まれる。接続要求を受信したセッション管理サーバ３は、端末１からの接続要求に関して、端末１が嘘をついていないことをチェックし（発信者詐称チェック）、更に、接続ポリシー制御機能を用いて端末１と端末２の接続が許可されているかをチェックし（ステップ８）、許可されていれば、名前解決機能を用いてデータベースを参照することにより端末２の名前から端末２のＩＰアドレスを取得し（ステップ９）、セキュアシグナリングチャネルを介して端末２へ接続要求を転送する（ステップ１０）。このとき、端末１のＩＰアドレスも端末２に送信される。端末１と端末２の接続が許可されていなければ、端末１の接続要求は拒否される。このとき、端末２に関する情報は端末１には全く送信されない。

【００３４】

接続要求を受信した端末２は、接続要求に対する応答として、暗号通信用の鍵情報を含む応答メッセージをセキュアシグナリングチャネルを介してセッション管理サーバ３に送信し（ステップ１１）、セッション管理サーバ３がその応答メッセージを端末１に送る（ステップ１２）。このとき、端末２のＩＰアドレスも端末１に送信される。

【００３５】

この手順により、端末１と端末２との間での暗号化通信が可能となる。すなわち、セキュアデータチャネルが確立され、所望のデータ通信が行われる。

【００３６】

ステップ１、２及び４、５を経てセキュアシグナリングチャネルが確立されているということは、端末－セッション管理サーバ間で相互に認証が成功しており、信頼関係が成立しているということである。端末１－セッション管理サーバ３間、及び端末２－セッション管理サーバ３間の各々でこのような関係が成立しているので、端末１と端末２との間も相互に信頼できる関係となることから、ステップ７以降は、一般の暗号化通信で用いられる鍵交換手順より簡略化した手順を用いることが可能となっている。

【００３７】

上記のシーケンスを実現する手段として、ＳＩＰ（session initiation protocol）を拡張したプロトコルを用いることが可能である。すなわち、セッション管理サーバ３をＳＩＰプロキシサーバとして機能させ、ＳＩＰのメッセージに上記の手順でやり取りされる情報を含ませる。

【００３８】

この場合、セキュアシグナリングチャネルの確立及び名前登録のためにＲＥＧＩＳＴＥＲメッセージを用い、端末１－端末２間のセキュアデータチャネル確立のためにＩＮＶＩＴＥメッセージを用いることができる。

【００３９】

ＳＩＰを用いる場合のシーケンス例を図３に示す。

【００４０】

図３に示す例は、セキュアなチャネルで接続された複数のセッション管理サーバを経由してシグナリングを行う場合の例である。なお、セキュアなチャネルで接続された複数のセッション管理サーバをセッション管理装置と称する場合がある。図３に示すシーケンスの構成において、端末１のＩＰアドレスが２００１：１２３４：：１０、セッション管理サーバＡのＩＰアドレスが２００１：６７８９：：５０６０、セッション管理サーバＢのＩＰアドレスが２００１：ａｂｃｄ：：５０６０、端末２のＩＰアドレスが２００１：ｃｄｅｆ：：１０である。

【００４１】

各端末とセッション管理サーバ間では予め互いにＩＤ、パスワードを配布しておき、端末とセッション管理サーバの各々は、相手のＩＤ、パスワードを自分の記憶装置に格納する。また、セッション管理サーバＡとセッション管理サーバＢの間は、ＴＬＳ等のセキュアなチャネルを介して通信を行う。

【００４２】

まず、端末１、２は、ＲＥＧＩＳＴＥＲメッセージを用いて、セッション管理サーバとのセキュアチャネルの確立、及び、（ＳＩＰに準拠した）名前の登録をセッション管理サーバＡ、Ｂに対して行う（ステップ２１）（図２のステップ１～６に相当する）。なお、この部分の手順については後により詳細に説明する。

【００４３】

続いて、端末１が、暗号通信用の鍵情報（図の例では秘密共有鍵生成用の情報）をＳＤＰパラメータとして記述したＩＮＶＩＴＥメッセージを、端末２への接続要求として、端末１とセッション管理サーバＡ間のセキュアシグナリングチャネルを介して送信する（ステップ２２）。セッション管理サーバＡは、そのＩＮＶＩＴＥメッセージをセッション管理サーバＡ、Ｂ間のセキュアなチャネルを介してセッション管理サーバＢに転送する（ステップ２３）。

【００４４】

なお、端末１からのＩＮＶＩＴＥメッセージにはRoute-Securityヘッダが含まれる。Route-Securityヘッダが付加されている場合、そのＩＮＶＩＴＥメッセージを受信した装置は、Route-Securityヘッダ：[アドレス]で示されているアドレスから当該装置までの経路がセキュアなものであるかとうか（例えばＩＰｓｅｃによる暗号化がなされているかどうか）をチェックし、セキュアなものであればそのRoute-Securityヘッダをそのまま残してメッセージを転送する。また、転送先で経路がセキュアなものであるかとうかチェックを要する場合には、Route-Securityヘッダ：[自分のアドレス]を付加したメッセージをその転送先に転送する。応答メッセージには、これまでに付されたRoute-Securityヘッダがそのまま付されており、これにより、メッセージがセキュアな経路を介して転送されたものであることがわかる。すわわち、Route-Securityヘッダにより、経路の安全性を担保する仕組みが提供される。

【００４５】

セッション管理サーバＢは端末２に、ＩＮＶＩＴＥメッセージを端末２とセッション管理サーバＢ間のセキュアシグナリングチャネルを介して送信する（ステップ２４）。なお、セッション管理サーバＡ及びセッション管理サーバＢにおいて端末２の名前解決がなされている。

【００４６】

ＩＮＶＩＴＥメッセージを受信した端末２は、暗号通信用の鍵情報をＳＤＰパラメータとして含む応答メッセージを端末１に向けて送信する（ステップ２５）。そして、その応答メッセージは、ＩＮＶＩＴＥメッセージと同じルート上を逆の方向に運ばれ、端末１に送信される（ステップ２６、２７）。

【００４７】

その後、受信確認（ＡＣＫ）メッセージが端末１から端末２に送信され（ステップ２８～３０）、端末１と端末２との間の暗号化通信（例えばＩＰｓｅｃによる通信）が可能となる。

【００４８】

図３のステップ２１におけるＲＥＧＩＳＴＥＲメッセージのシーケンスは、例えば図４に示す通りである。

【００４９】

この場合、まず、暗号通信用（ＩＰｓｅｃ等）の鍵情報を含むＲＥＧＩＳＴＥＲメッセージを端末からセッション管理サーバに送信する（ステップ２１１）。セッション管理サーバはその応答として暗号通信用の鍵情報を含む応答メッセージを端末に返す（ステップ２１２）。続いて、端末は、セッション管理サーバが端末を認証するための認証用情報を含むＲＥＧＩＳＴＥＲメッセージをセッション管理サーバに送信する（ステップ２１３）。セッション管理サーバはその応答として、端末がセッション管理サーバを認証するために必要な認証用情報を含む応答メッセージを端末に送信する（ステップ２１４）。互いの認証が取れた後、セキュアシグナリングチャネルによる暗号化通信が可能となる。

【００５０】

その後は、パケットがセキュアシグナリングチャネルを介して暗号化して送受信されるため、通常のＲＥＧＩＳＴＥＲメッセージシーケンスにより名前の登録が行われる（ステップ２１５、２１６）。

【００５１】

なお、上記のシーケンスにおいて、ＩＰｓｅｃ等の暗号化通信に必要なその他の情報は適宜送受信されているものとする。なお、認証用情報は、ＩＤ、パスワード等を含む情報でもよいし、証明書（Ｘ．５０９証明書等）でもよい。また、暗号通信用の鍵情報の交換のために用いるメッセージに認証用情報（証明書）を含めてもよい。

【００５２】

次に、シグナリングプロトコルとしてＳＩＰを用いる場合の各装置の機能ブロックを図５を参照して説明する。

【００５３】

セッション管理サーバは、呼（メッセージ）の転送のための処理を行うＳＩＰプロキシ、ＳＩＰの名前登録を行うＳＩＰレジストラ、ＩＤ、パスワード、もしくは証明書等を用いて各端末の認証を行う認証モジュール、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュールを有している。

【００５４】

また、各端末は、セキュアデータチャネル上での通信を行う機能部、ＩＮＶＩＴＥメッセージの送受信やＲＥＧＩＳＴＥＲメッセージの発行等を含むＳＩＰに基づくメッセージ通信を行うＳＩＰ機能部、ＩＤ、パスワード、もしくは証明書等を用いてセッション管理サーバの認証を行う認証モジュール、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュールを有している。

【００５５】

上記のセッション管理サーバ、各端末の機能は、プログラムにより実現されるものであり、本発明におけるセッション管理装置、端末の各手段は、プログラムと、セッション管理装置、端末のハードウェアとで実現されているものである。また、端末は、ＣＰＵ、メモリ、ハードディスク等を含む一般的なＰＣ等のコンピュータ、モバイル機器等であり、当該コンピュータ等に上記プログラムをインストールすることにより本実施の形態の端末の機能を実現できる。なお、端末はディジタル家電等でもよい。また、セッション管理サーバは、サーバ等のコンピュータであり、当該サーバに上記プログラムをインストールすることにより本実施の形態のセッション管理サーバの機能を実現できる。

【００５６】

上記のように本実施の形態のような構成としたことにより、次のような効果を奏する。

【００５７】

まず、端末のアドレスが変更される度にＲＥＧＩＳＴＥＲメッセージによる名前とＩＰアドレスの登録を行うので、端末側はいわゆる動的ＩＰアドレス割り当てを用いることができる。また、セッション管理サーバが名前解決を行うことから、従来は必要であったオープンなＤＮＳへの名前登録が不要となる。また、各端末とセッション管理サーバ間でセキュアなチャネルを構築してシグナリングを行うので、端末側でのＦＷ管理が不要となる。また、セッション管理サーバが各端末のＩＤ、パスワードを管理するので、端末側で多数のＩＤ、パスワードを管理することが不要となる。また、セッション管理サーバ接続ポリシー制御機能により、接続を許可していない相手端末に対しては、名前解決さえ許可していないので、その端末の存在自体を知られることがなく、端末が不正なアクセスを受ける恐れがなくなる。更に、セキュアシグナリングチャネルを介したシグナリングにより、セキュアデータチャネルに必要なポート番号が伝えられるので、シグナリングが正常に完了しない場合には、外部にはポート番号を知られることがない。また、軽いシグナリングだけが中間サーバ（セッション管理サーバ）を経由し、実際のデータ通信は端末間でピア・ツー・ピアで行われるので、中間サーバの負荷が過大となることはない。

【００５８】

また、従来技術においては、多数の端末同士の間で相互認証および暗号化されたピア・

ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のＩＤ、パスワードを管理することが必要であったが、本発明によれば、メンバー同士であれば何の事前セキュリティ設定が不要となる。

【００５９】

また、従来技術において、データチャネルの暗号化が不要だったとしても、発番号の信憑性を確保する手段として、PKIを使う方法等しかなかったが、本発明によれば、サービス設定（SIPのID/パスワード設定）だけで発番号の詐称・改竄を防ぐことができる。

【００６０】

（第２の実施の形態）

次に、上述したような、各端末とセッション管理サーバとの間でセキュアシグナリングチャネルを用いて、ＳＩＰメッセージに暗号化通信のために必要な鍵情報を含めて送るというしくみを応用した実施の形態を説明する。

【００６１】

ＳＳＬによる暗号通信のように公開鍵ベースの認証技術を用いる場合、認証機関（ＣＡ）から発行される公開鍵証明書を用いることが必要であるが、ＣＡから公開鍵証明書を受けたり、それを定期的に更新することは煩雑であり、公開鍵証明書を用いた公開鍵ベースの認証技術の利用は敬遠される場合が多かった。

【００６２】

以下で説明する第２の実施の形態では、各端末とセッション管理サーバとの間に信頼関係が確立されることを利用して、端末から公開鍵を簡易にサーバに登録し、そのサーバから簡易にその公開鍵の公開鍵証明書や公開鍵自身を取得できるようにしている。これにより、端末間で容易に公開鍵ベースの認証技術の利用ができ、ＳＳＬ等の暗号通信を端末間で容易に行うことができる。

【００６３】

図６～図８を用いて、本実施の形態における通信手順について説明する。

【００６４】

本実施の形態におけるシステム構成は、公開鍵を配布する側の端末１１と、その公開鍵の配布を受けて、端末１１と公開鍵ベースの暗号通信を行う端末１２と、第１の実施の形態と同様の機能を含むセッション管理サーバ２１、セッション管理サーバ２２、及び、セッション管理サーバ２１、２２とセキュアなチャネルで接続された簡易ＣＡサーバ３０を有するものである。また、各端末とセッション管理サーバ間は、第１の実施の形態で説明した方法により、セキュアシグナリングチャネルが確立されている。なお、セッション管理サーバと簡易ＣＡサーバは１つの装置として構成することもできる。また、セキュアなチャネルで接続された簡易ＣＡサーバとセッション管理サーバをまとめて公開鍵管理装置と称する場合がある。

【００６５】

また、本実施の形態では、各端末、セッション管理サーバ２１、２２、簡易ＣＡ管理サーバ３０は、公開鍵証明書の発行を要求するためのＰＵＢＬＩＳＨメッセージ（ＳＩＰメッセージ）を送受信する機能を有している。ＰＵＢＬＩＳＨメッセージは、そのボディ部に公開鍵、公開鍵証明書等を記述して用いる。

【００６６】

図６において、まず、端末１１は秘密鍵と公開鍵のペアを作成する（ステップ３１）。そして、端末１１とセッション管理サーバ２１間のセキュアシグナリングチャネル、及びセッション管理サーバと簡易ＣＡサーバ間のセキュアチャネルを介し、ＰＵＢＬＩＳＨメッセージを用いて公開鍵を簡易ＣＡサーバに登録する（ステップ３２）。

【００６７】

続いて、図７において、端末１１が簡易ＣＡサーバ３０から、セッション管理サーバ２１及びセキュアシグナリングチャネルを介して、簡易ＣＡサーバ３０の秘密鍵を用いて作成された公開鍵証明書を取得する（ステップ３３）。公開鍵証明書は、例えば、予め定め

た一定の期間のみ簡易ＣＡサーバ３０から発行される。なお、この予め定めた一定の期間が、公開鍵証明書の有効期間と一致する。そして、図８に示すように、端末１１は、一般の端末１３に公開鍵証明書を配布することにより（ステップ３４）、例えば、端末１１と端末１３間でのＳＳＬ通信が可能となる。なお、端末１１と端末１３間で公開鍵を用いてＳＳＬ通信を行う方法は従来のＳＳＬ通信の方法と同じである。

【００６８】

また、簡易ＣＡサーバ３０とセキュアに接続され、簡易ＣＡサーバ３０と信頼関係にある端末１２は、端末１１の公開鍵を公開鍵証明書という形式にせずに簡易ＣＡサーバ３０から受信できる（ステップ３５）。そして、端末１１と端末１２間で公開鍵ベースの暗号通信を行うことが可能となる。

【００６９】

端末１１と端末１３間でセキュアデータチャネル（ＳＳＬ通信チャネル）を構築する場合におけるシーケンスを図９に示す。なお、図９には、セッション管理サーバ２２を図示していない。

【００７０】

端末１１とセッション管理サーバ２１において、ＲＥＧＩＳＴＥＲメッセージによりセキュアシグナリングチャネルを確立し、ＳＩＰ名前登録を行うまでの手順（ステップ４１）は、第１の実施の形態と同じである。また、セッション管理サーバ２１と簡易ＣＡサーバ３０間はＴＬＳセキュアチャネルにより接続されている。また、端末１３は、簡易ＣＡサーバ３０自身の公開鍵を予め取得しているものとする。

【００７１】

端末１１は、端末１１の公開鍵を登録するために、まず公開鍵をＳＩＰボディ部に含むＰＵＢＬＩＳＨメッセージをセッション管理サーバ２１に送信する（ステップ４２）。セッション管理サーバ２１はＰＵＢＬＩＳＨメッセージを簡易ＣＡサーバ３０に転送する（ステップ４３）。簡易ＣＡサーバ３０は、公開鍵の登録及び公開鍵証明書の発行を行い、ＰＵＢＬＩＳＨメッセージへの応答として、公開鍵証明書をボディ部に含む応答メッセージをセッション管理サーバ２１に送信し（ステップ４４）、セッション管理サーバ２１がその応答メッセージを端末１１に転送する（ステップ４５）。その後、端末１１と端末１３間でＳＳＬ暗号化通信のためのセッションを開始する（ステップ４６～）。ステップ４６以降は、従来のＳＳＬ通信を行うための手順と同じである。すなわち、ステップ４５までの処理を予め行っておくことにより、それ以降の任意のタイミングで端末間のＳＳＬ通信を自由に行うことができる。

【００７２】

図１０に各装置の機能ブロック図を示す。

【００７３】

セッション管理サーバの機能は第１の実施の形態と同様である。端末は、図５に示した機能に加えて、ＳＩＰ機能部内に、ＰＵＢＬＩＳＨメッセージの送信機能を有している。また、秘密鍵、公開鍵の生成機能及び公開鍵証明書の管理機能を有している。また、簡易ＣＡサーバは、暗号化モジュール、認証モジュール、ＳＩＰ機能部に加えて、公開鍵の管理や公開鍵証明書の発行を行う機能を有している。公開鍵の管理とは、例えば、公開鍵を、その公開鍵に対応する端末の識別情報とともに記憶装置に格納することである。

【００７４】

上記のように、本実施の形態によれば、端末とセッション管理サーバ及び簡易ＣＡサーバとの信頼関係をもとに、簡易な公開鍵管理モデルを実現できる。

【００７５】

上記の各実施の形態では、ＳＩＰを情報送受信の手段として用いる場合を例にとって説明しているが、情報送受信の手段としてはＳＩＰに限定されるものではない。例えば、ＳＩＰに代えてＨＴＴＰを用いることができる。

【００７６】

（第３の実施の形態）

セキュアシグナリングチャネルを利用したシグナリングによりセキュアデータチャネルを構築するしくみを応用した更なる実施の形態を次に説明する。なお、以下の説明において、“ｈｔｔｐ”は、特に示していない場合には、“ｈｔｔｐｓ”を含む広い意味で使用する。

【００７７】

本実施の形態は、図２の構成における一方の端末（例えば端末１）に、ｈｔｔｐからＳＩＰへのプロトコル変換を行うゲートウェイ機能（以下、端末１をゲートウェイ装置１と呼ぶ）を備え、携帯電話、ＰＤＡ等のモバイル端末がゲートウェイ装置１にアクセスすることにより、モバイル端末と端末２間でのセキュアなデータチャネルによる通信を可能とする形態である。

【００７８】

図１１に、本実施の形態の全体構成を示す。図１１に示すように、図２に示す構成における端末１をゲートウェイ装置１に置き換え、モバイル端末４１や、社内のファイアウォール配下にあるＷｅｂブラウザ端末４２等がゲートウェイ装置１にアクセスし、ゲートウェイ装置１と端末２間でセキュアデータチャネルが構築され、ゲートウェイ装置１を介してモバイル端末４１等と端末２間で通信を行う。なお、端末２は、例えば特定のユーザからのアクセスのみを許容するＷｅｂサーバである。

【００７９】

次に、図１２のシーケンスチャートを参照して、本実施の形態の動作を説明する。なお、図１２のシーケンスにおいて、ゲートウェイ装置１とセッション管理サーバ３間、及びセッション管理サーバ３と端末２間におけるセキュアシグナリングチャネルは構築済みであるものとする。以下、ゲートウェイ装置１にアクセスする端末として、モバイル端末４１を例にとり説明する。

【００８０】

まず、モバイル端末４１がｈｔｔｐプロトコルを用いてゲートウェイ装置１にアクセスする（ステップ５１）。アクセスの際、ゲートウェイ装置１は、モバイル端末４１の電話番号を取得する。また、モバイル端末４１からゲートウェイ装置１に、ＩＤとパスワードを送信するようにしてもよい。ゲートウェイ装置１は、電話番号、もしくはＩＤ、パスワードによりモバイル端末４１の認証を行う（ステップ５２）。

【００８１】

ゲートウェイ装置１は、図１３に示すような、ユーザ識別子（電話番号やＩＤ）と、そのユーザに接続許容されている接続先の名前を格納するテーブルを保持している。例えば、ゲートウェイ装置１は、モバイル端末４１からのアクセスを受けて、当該テーブルから名前を取得し、モバイル端末４１にそれを送信する。モバイル端末４１では、その名前を表示し、ユーザに特定の名前を選択させ、選択された名前をゲートウェイ装置１に送信する。これにより、ゲートウェイ装置１は、モバイル端末４１のアクセス先の名前を取得することができる。このような方法に代えて、モバイル端末４１から直接名前を入力してゲートウェイ装置１に送信するようにしてもよい。また、モバイル端末４１で表示するものを、名前そのものではなくその名前に対応したサイトの概要を示す画像としてもよい。

【００８２】

上記のようにして名前を取得したゲートウェイ装置１は、その名前を含むＩＮＶＩＴＥメッセージをセッション管理サーバ３に送信することにより、その名前が示す接続先（本実施の形態では端末２）への接続要求を行う。図１２に示すステップ５３～５６の処理は、図２のステップ７～１２に示す処理と同じである。

【００８３】

セキュアデータチャネル確立の後、ステップ５９において、モバイル端末４１にｈｔｔｐレスポンスが返される。その後、モバイル端末４１とゲートウェイ装置１との間、及びゲートウェイ装置１と端末２との間でｈｔｔｐプロトコル、もしくはｈｔｔｐｓプロトコル等による通信が行われる。ここでは、ゲートウェイ装置１が端末２からデータを受け、それをモバイル端末４１に送信する動作を行う。また、必要に応じて、モバイル端末４１

への表示に適するように、ゲートウェイ装置１にてデータ変換が行われる。また、モバイル端末４１からのリクエストをゲートウェイ装置１が受け、それを端末２に送信している。

【００８４】
上記の例ではゲートウェイ装置１とセッション管理サーバ３間に共通のセキュアシグナリングチャネルが予め構築されているものとしたが、モバイル端末４１によるアクセスに応じて、当該モバイル端末４１用に、ゲートウェイ装置１とセッション管理サーバ３間にセキュアシグナリングチャネルを設けてもよい。

【００８５】
図１４に、ゲートウェイ装置１の機能ブロック図を示す。なお、図１４は、データチャネル構築のためのシグナリングをするための機能を主に示している。

【００８６】
図１４に示すように、ゲートウェイ装置１は、ｈｔｔｐプロトコル処理を行うＷｅｂサーバ部５１、擬似ＳＩＰ機能部５２、ＳＩＰ制御部５３、ＩＰｓｅｃ制御部５４、モバイル端末の認証等のために用いるデータベース５５を備えている。また、図示していないが、セキュアデータチャネル確立後にゲートウェイ装置１と端末２間でｈｔｔｐ通信を行うためのｈｔｔｐプロトコル処理部を備えている。

【００８７】
擬似ＳＩＰ機能部５２は、擬似ＳＩＰ機能制御部５２１を有しており、モバイル端末４１からのアクセスに応じて個別擬似ＳＩＰ機能部５２２を生成する。個別擬似ＳＩＰ機能部５２２は、アクセスしてきたモバイル端末に代わって、セキュアシグナリングデータチャネル確立のためのシグナリングを行うためのものである。擬似ＳＩＰ機能部５２は、モバイル端末に代わって擬似的に、図２等に示した端末におけるＳＩＰ機能部としての役割を果たすことから、“擬似”ＳＩＰ機能部と称している。個別擬似ＳＩＰ機能部５２２では、ＳＩＰメッセージに含める実質的な情報を生成してＳＩＰ制御部５３に渡し、ＳＩＰ制御部５３がＳＩＰプロトコルに従ったパケットを生成して、送信している。ＩＰｓｅｃ制御部５４は、図５に示す暗号化モジュールに相当する。

【００８８】
次に全体の動作を説明する。なお、ゲートウェイ装置１とセッション管理サーバ３間におけるセキュアシグナリングチャネルの構築は、ＳＩＰ制御部５３により既に行われているものとする。なお、モバイル端末とゲートウェイ装置間の通信はｈｔｔｐ、ｈｔｔｐｓのいずれでもよい。

【００８９】
まず、モバイル端末４１からのｈｔｔｐリクエストをＷｅｂサーバ部５１が受信する。Ｗｅｂサーバ部５１は、ｈｔｔｐリクエストの情報を擬似ＳＩＰ機能制御部５２１に渡す。擬似ＳＩＰ機能制御部５２１は、その情報に含まれるＩＤ等の情報を用い、データベース５５を参照することによりアクセスしてきたモバイル端末４１の認証を行う。認証がＯＫであれば、アクセスしてきたモバイル端末４１に対応する個別擬似ＳＩＰ機能部５２２を生成する。そして、例えば前述したような接続先名前取得手順により、モバイル端末４１のユーザが希望する接続先の名前を取得する。なお、図１３に示すテーブル情報はデータベース５５に含まれる。

【００９０】
その後、個別擬似ＳＩＰ機能部５２２は、接続要求となるＩＮＶＩＴＥメッセージを生成し、ＳＩＰ制御部５３を介してセッション管理サーバ３に送信する。そして、図１２に示すシーケンスにより、ＩＰｓｅｃ制御部５４が、端末２との間でのＩＰｓｅｃコネクション（セキュアデータチャネル）を作成する。これにより、これ以降、セキュアデータチャネルを介してゲートウェイ装置１と端末２との間で、例えばｈｔｔｐもしくはｈｔｔｐｓによる通信を行うことができる。そして、ゲートウェイ装置１が受信したデータは、必要に応じて変換されてモバイル端末４１に送信される。

【００９１】

以上説明したように、本実施の形態によれば、ゲートウェイ装置１が、モバイル端末４１等の代わりとしての擬似ＳＩＰ機能を備え、モバイル端末４１の代わりにセキュアデータチャネル構築のためのシグナリングを行う。

【００９２】

従って、ｈｔｔｐ通信のみの機能を持つ端末でも、接続相手側がＳＩＰに基づく通信によりチャネルを確立する端末であることを全く意識せずに、従来のｈｔｔｐ接続をゲートウェイ装置１に対して行うだけで、接続相手の端末とセキュアデータチャネルを用いたセキュアな通信を行うことが可能となり、第１の実施の形態で説明したしくみの適用範囲がより広くなる。

【００９３】

また、ゲートウェイ装置１に、各端末が接続可能な相手先を格納した図１３に示すようなテーブルを保持することにより、携帯電話などの操作系が貧弱な端末でも、ゲートウェイのポータルサイトにアクセスして相手先を選択するだけで、相手方への簡易な接続が可能となる。

【００９４】

本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【図面の簡単な説明】

【００９５】

【図１】本発明の第１の実施の形態の概要について説明するための図である。

【図２】端末１－セッション管理サーバ３－端末２間の通信のシーケンス図である。

【図３】シーケンスを詳細に示す図である。

【図４】ＲＥＧＩＳＴＥＲメッセージのシーケンスを示す図である。

【図５】シグナリングプロトコルとしてＳＩＰを用いる場合の各装置の機能ブロック図である。

【図６】第２の実施の形態における通信手順を説明するための図である。

【図７】第２の実施の形態における通信手順を説明するための図である。

【図８】第２の実施の形態における通信手順を説明するための図である。

【図９】端末１１と端末１３間でセキュアデータチャネル（ＳＳＬ通信チャネル）を構築する場合におけるシーケンス図である。

【図１０】第２の実施の形態における各装置の機能ブロック図である。

【図１１】第３の実施の形態におけるシステム構成図である。

【図１２】第３の実施の形態の動作を示すシーケンスチャートである。

【図１３】ユーザと接続先の対応を示すテーブルである。

【図１４】ゲートウェイ装置１の機能ブロック図である。

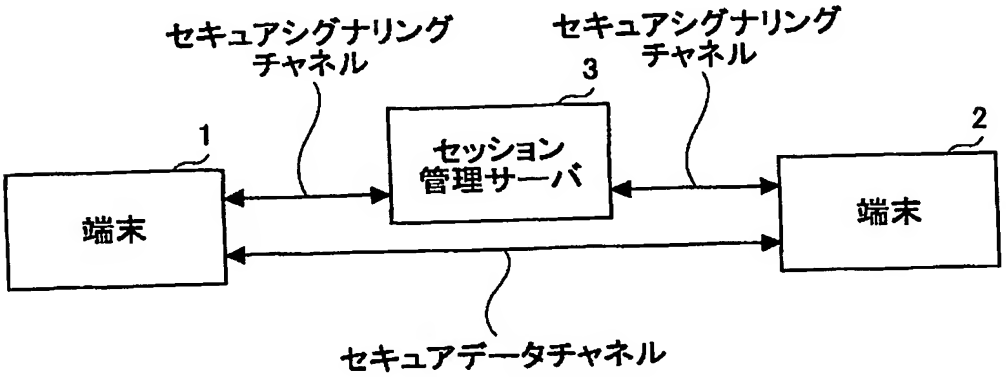
【符号の説明】

【００９６】

１、２、１１、１２、１３　端末
３、Ａ、Ｂ、２１、２２　セッション管理サーバ
３０　簡易ＣＡサーバ
４１　モバイル端末
４２　ＦＷ配下Ｗｅｂブラウザ端末
５１　Ｗｅｂサーバ部
５２　擬似ＳＩＰ機能部
５３　ＳＩＰ制御部
５４　ＩＰｓｅｃ制御部
５５　データベース
５２１　擬似ＳＩＰ機能制御部
５２２　個別擬似ＳＩＰ機能部

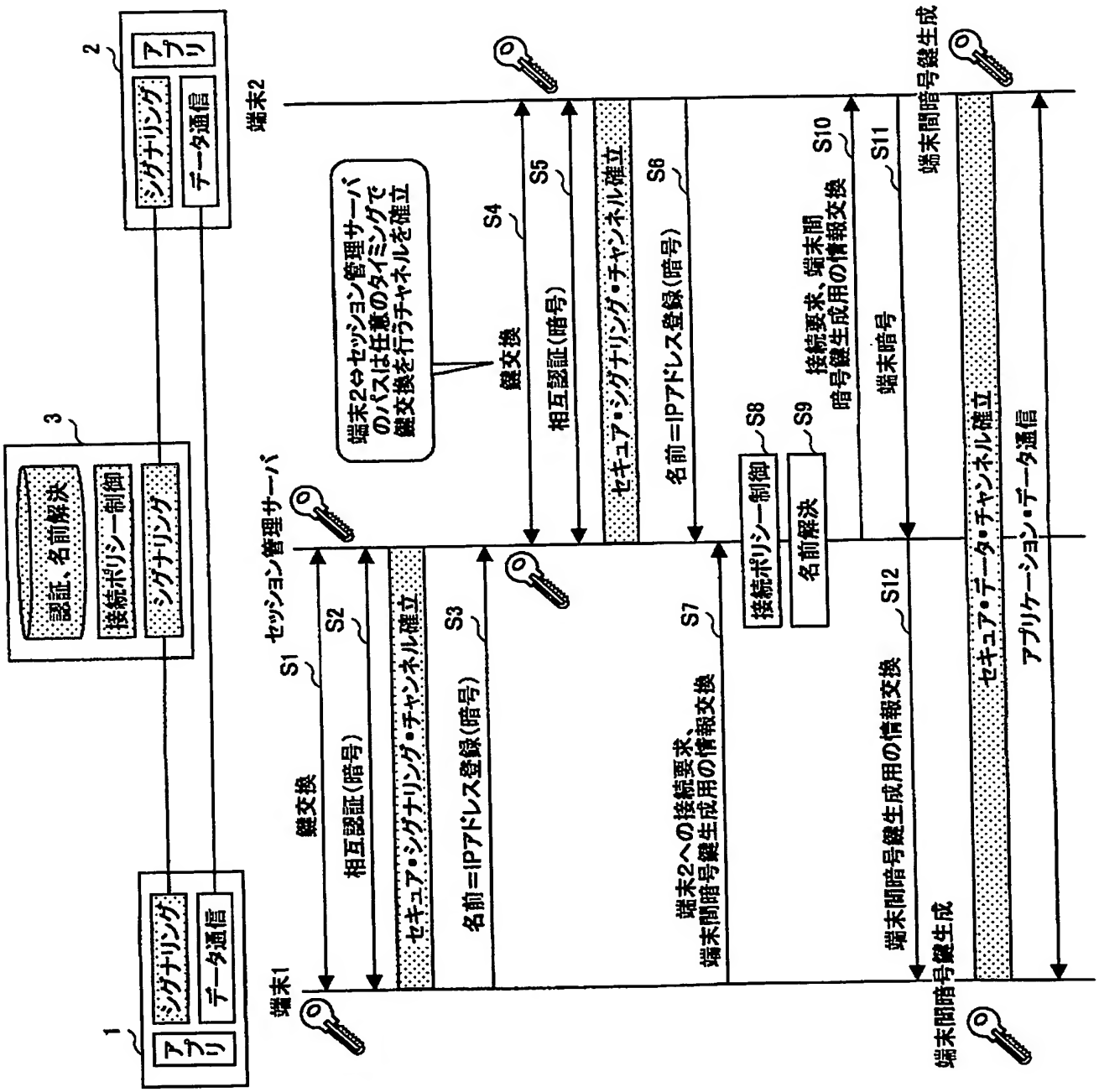
【書類名】図面
【図１】

本発明の第1の実施の形態の概要について説明するための図



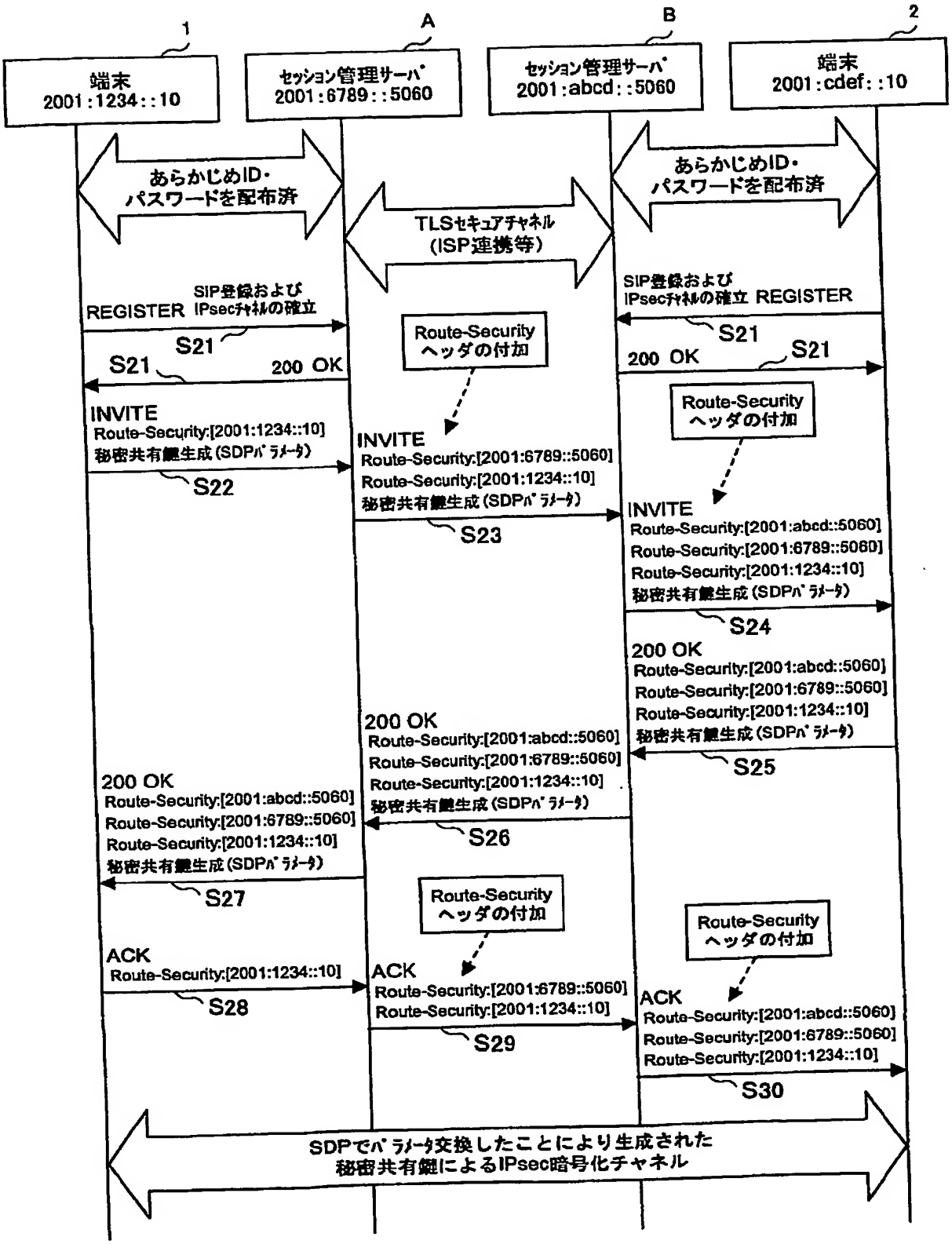
【図２】

端末1－セッション管理サーバ3－端末2間の通信のシーケンス図



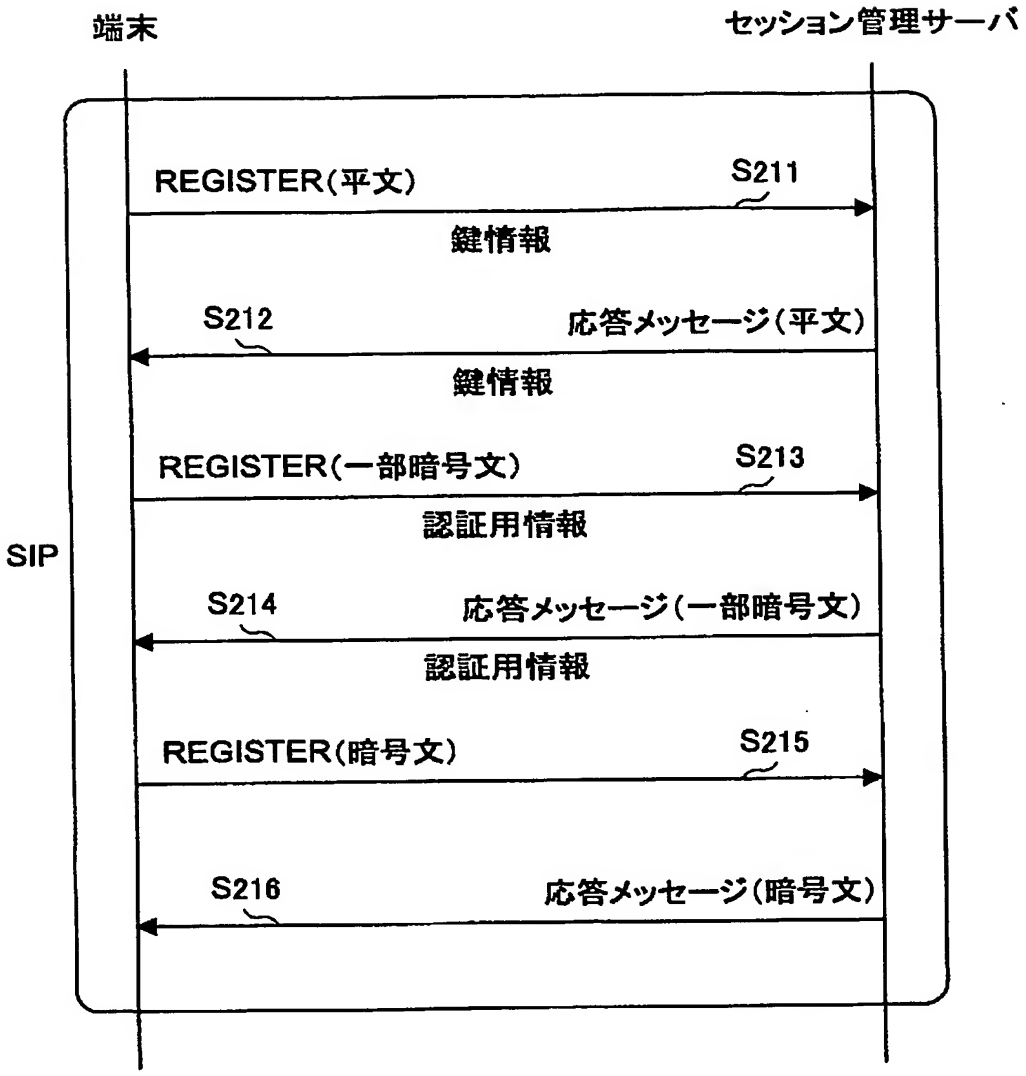
【図３】

シーケンスを詳細に示す図



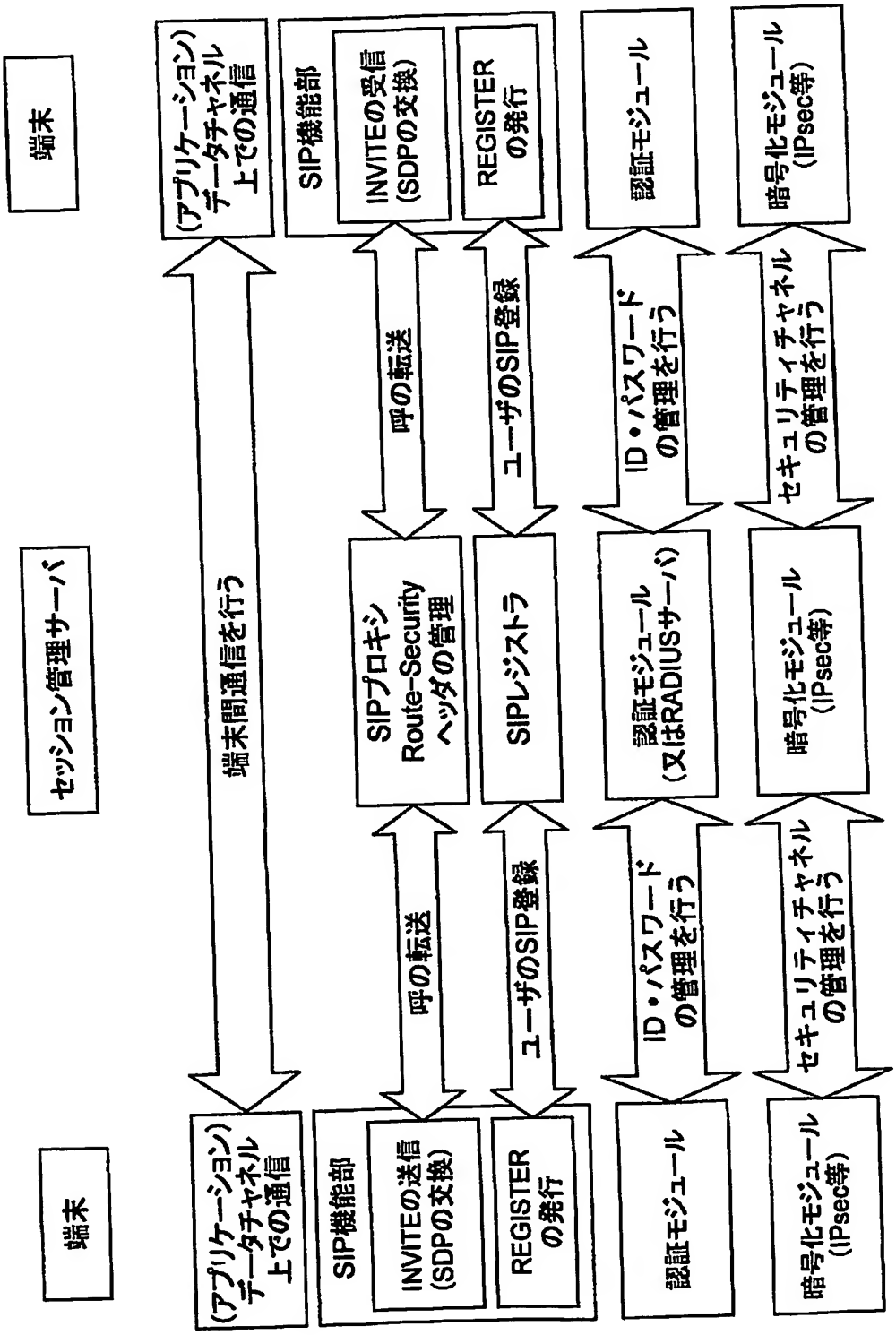
【図４】

REGISTERメッセージのシーケンスを示す図



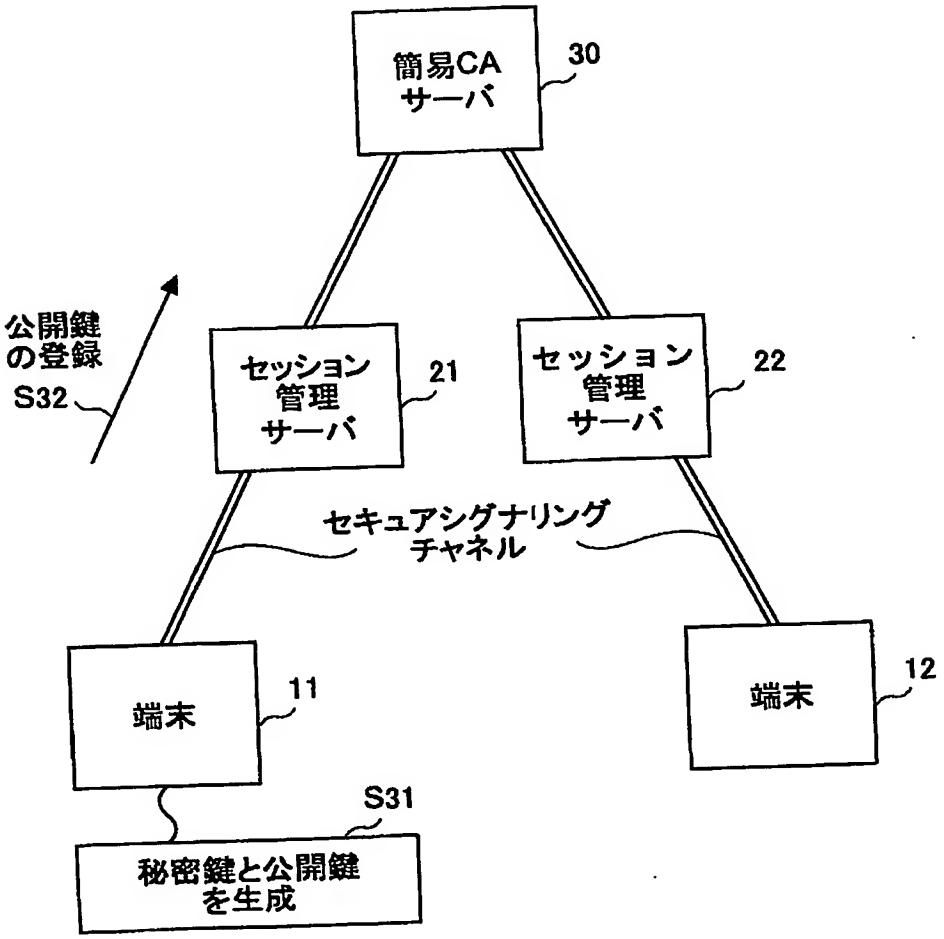
【図５】

シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロック図



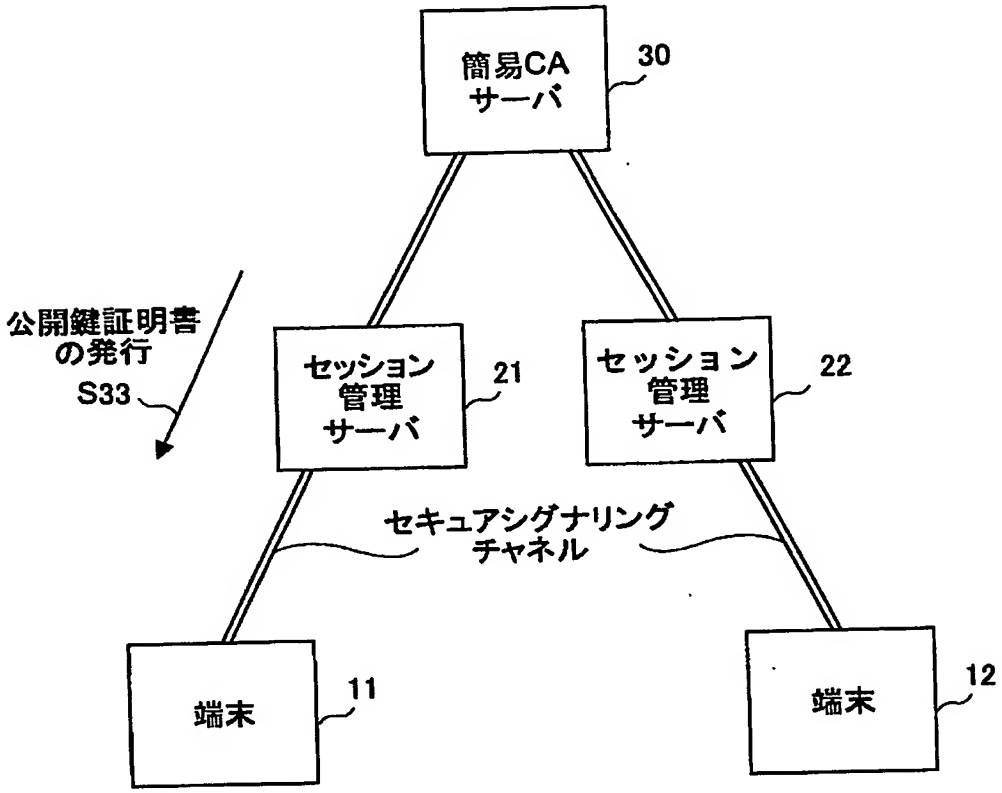
【図６】

第2の実施の形態における通信手順を説明するための図



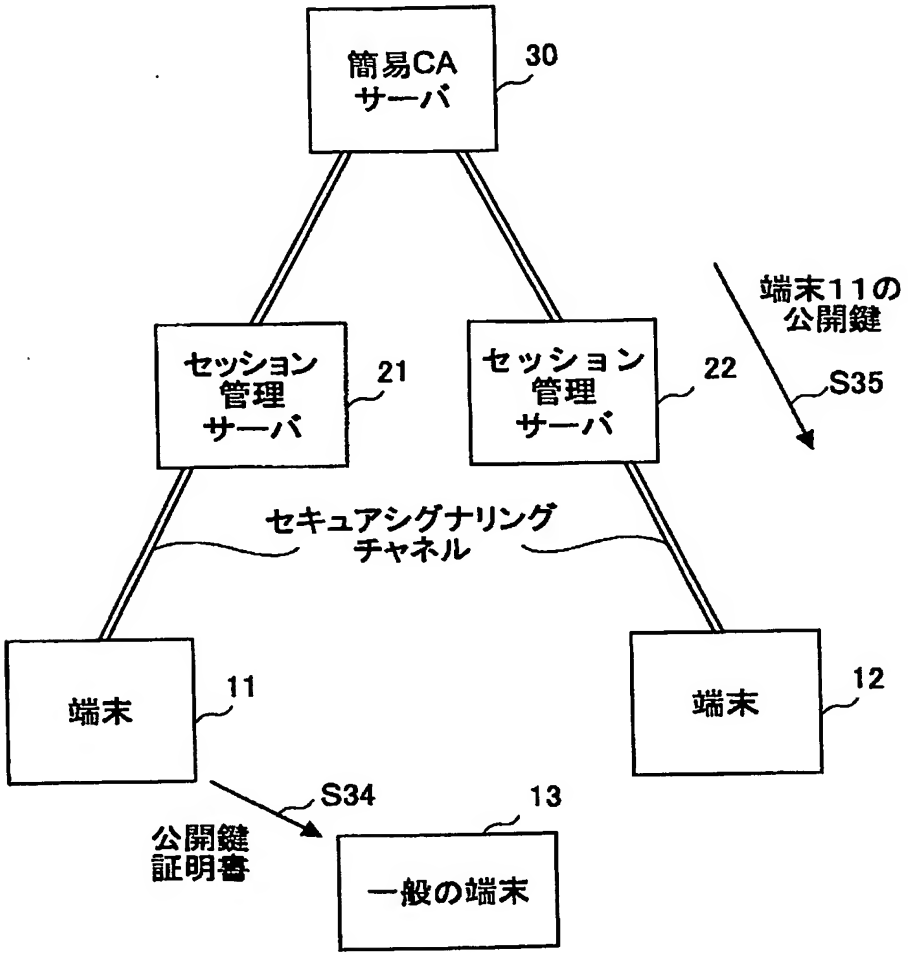
【図７】

第2の実施の形態における通信手順を説明するための図



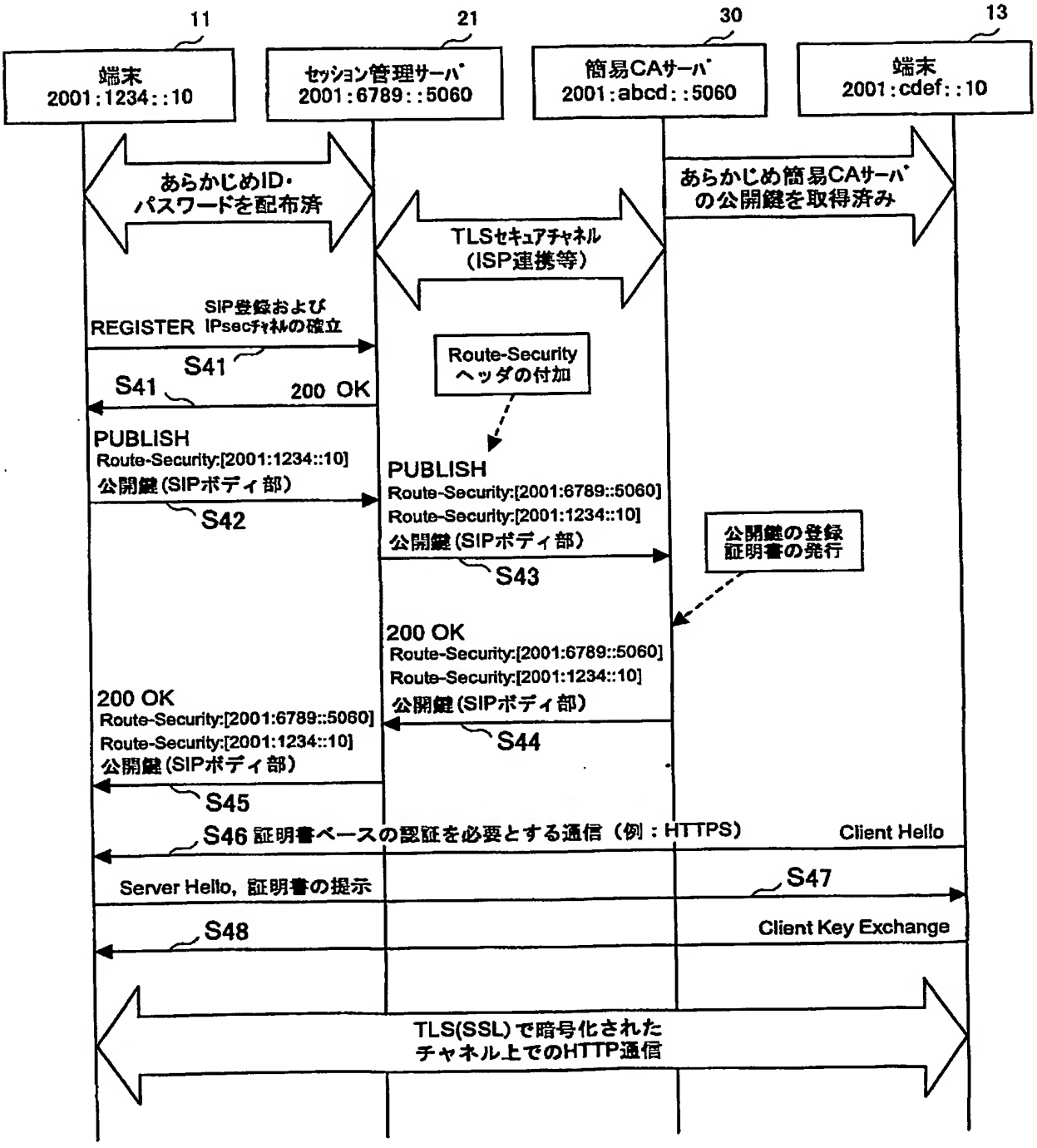
【図８】

第2の実施の形態における通信手順を説明するための図



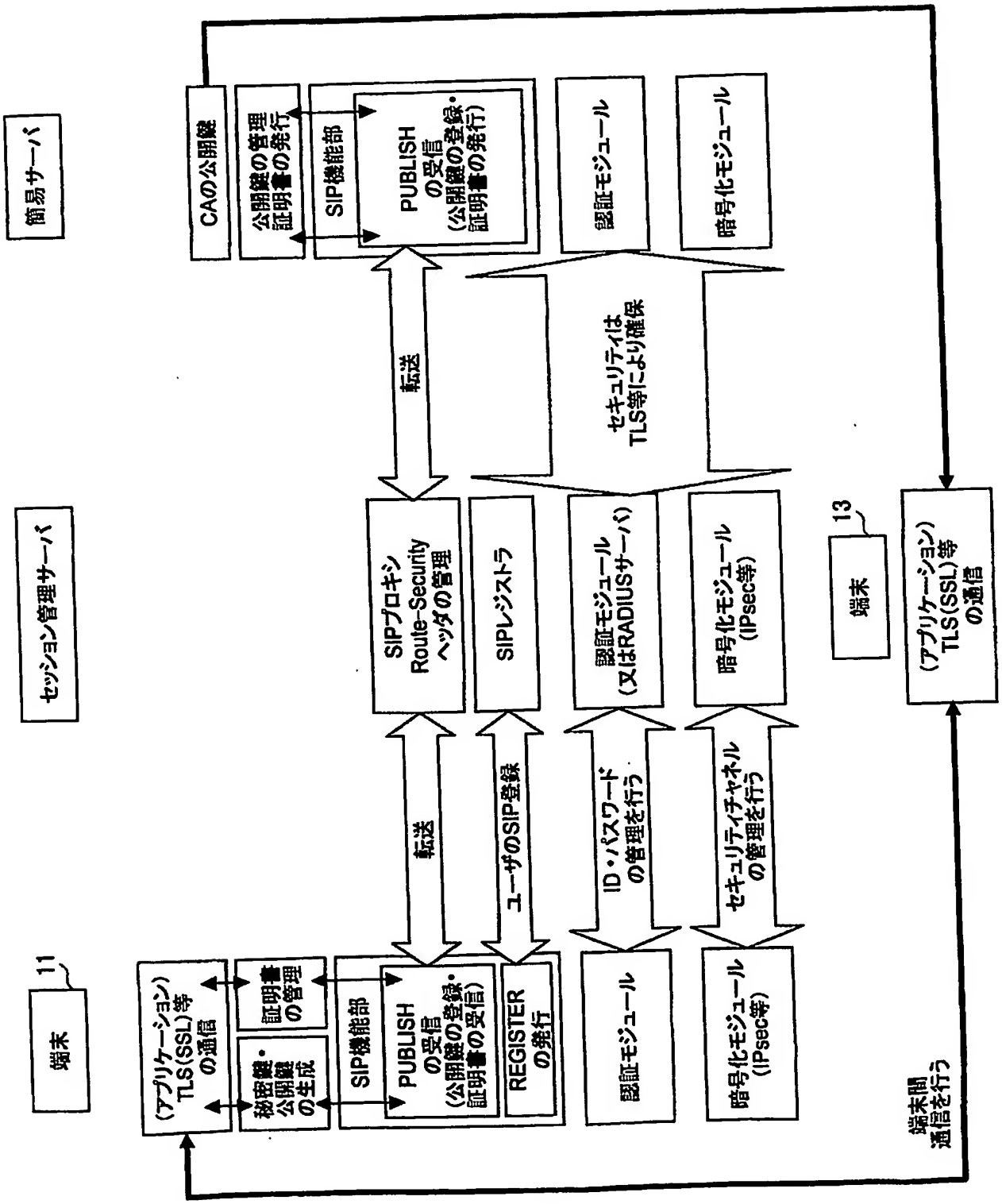
【図９】

端末11と端末13間でセキュアデータチャネル（SSL通信チャネル）を構築する場合におけるシーケンス図



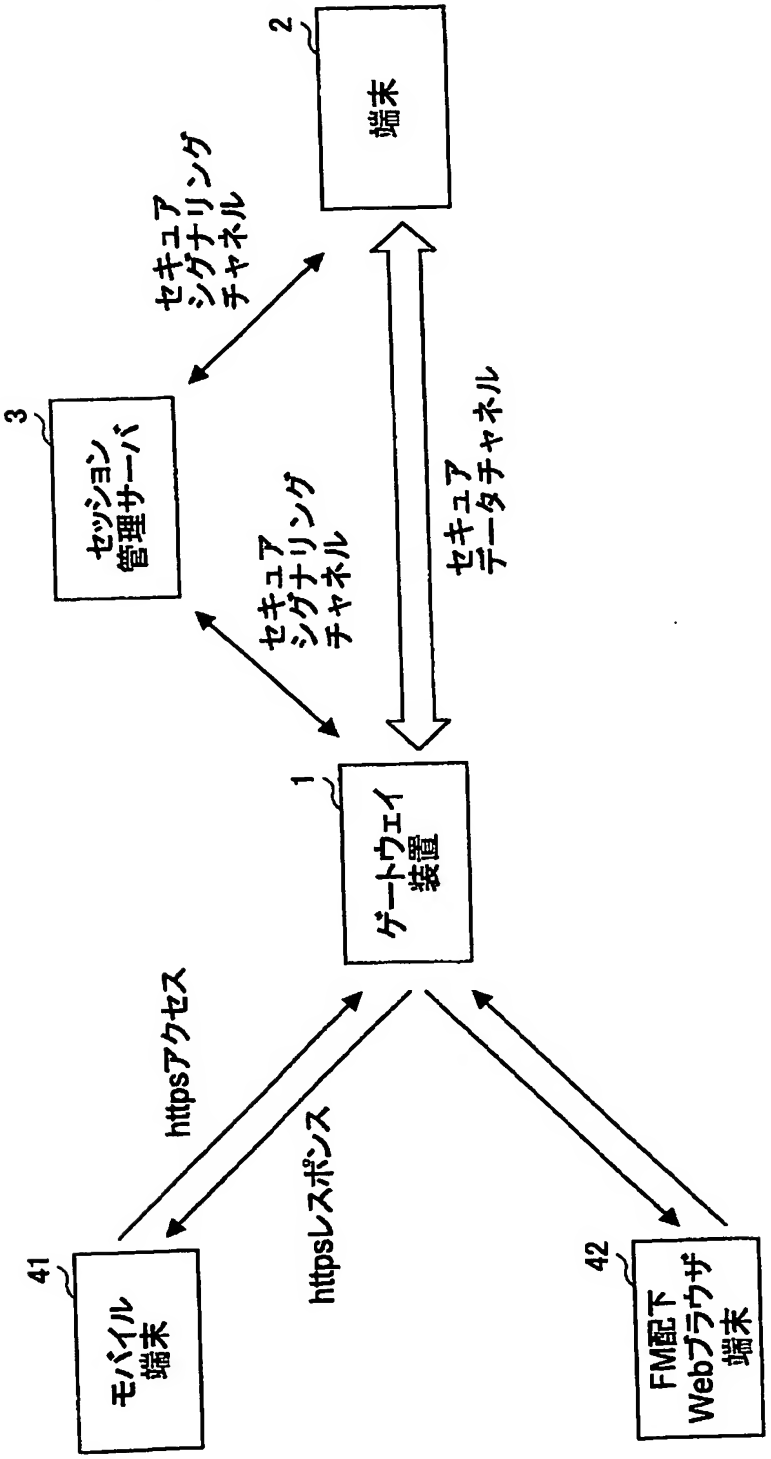
【図１０】

第2の実施の形態における各装置の機能ブロック図



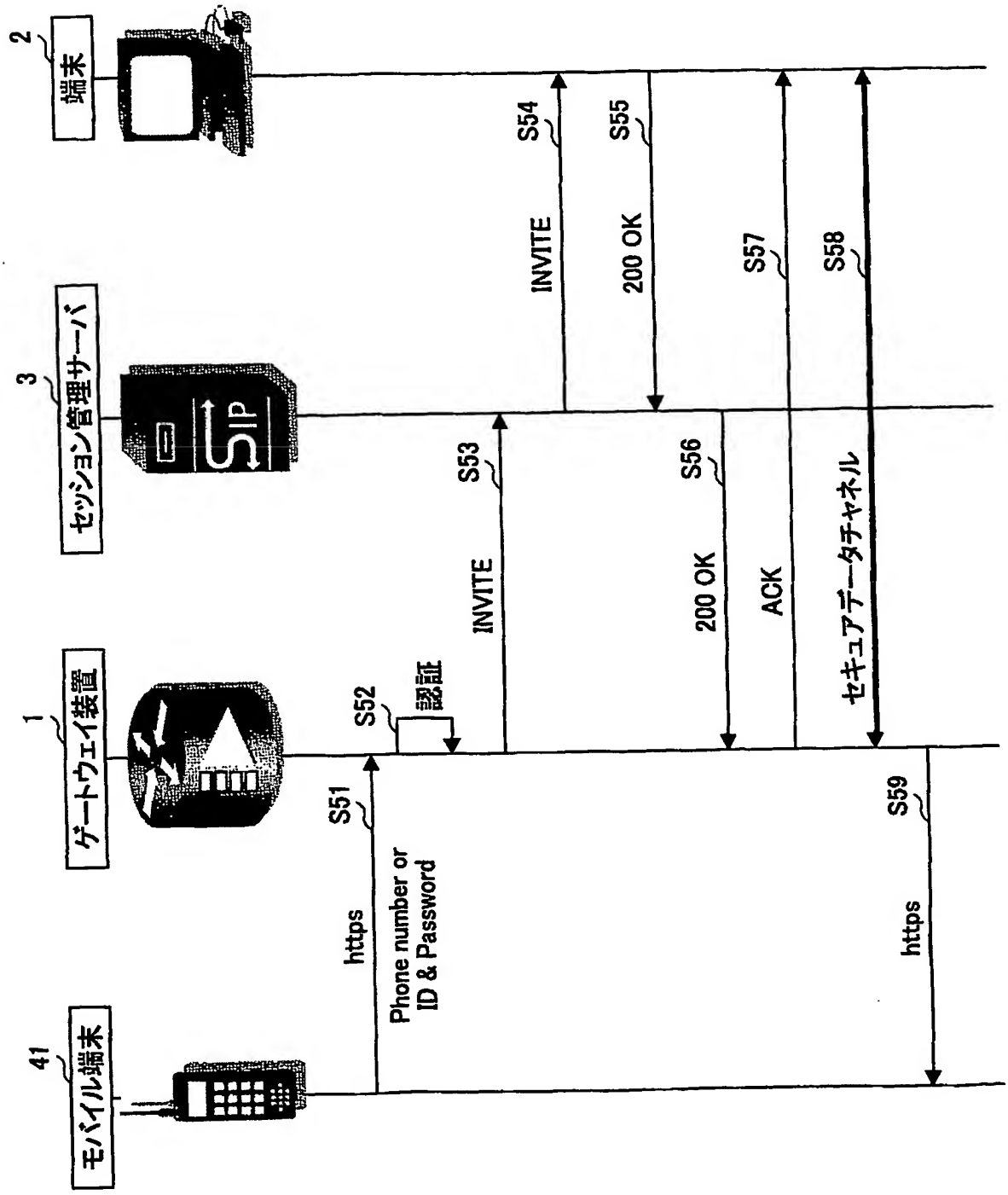
【図１１】

第3の実施の形態におけるシステム構成図



【図１２】

第3の実施の形態の動作を示すシーケンスチャート



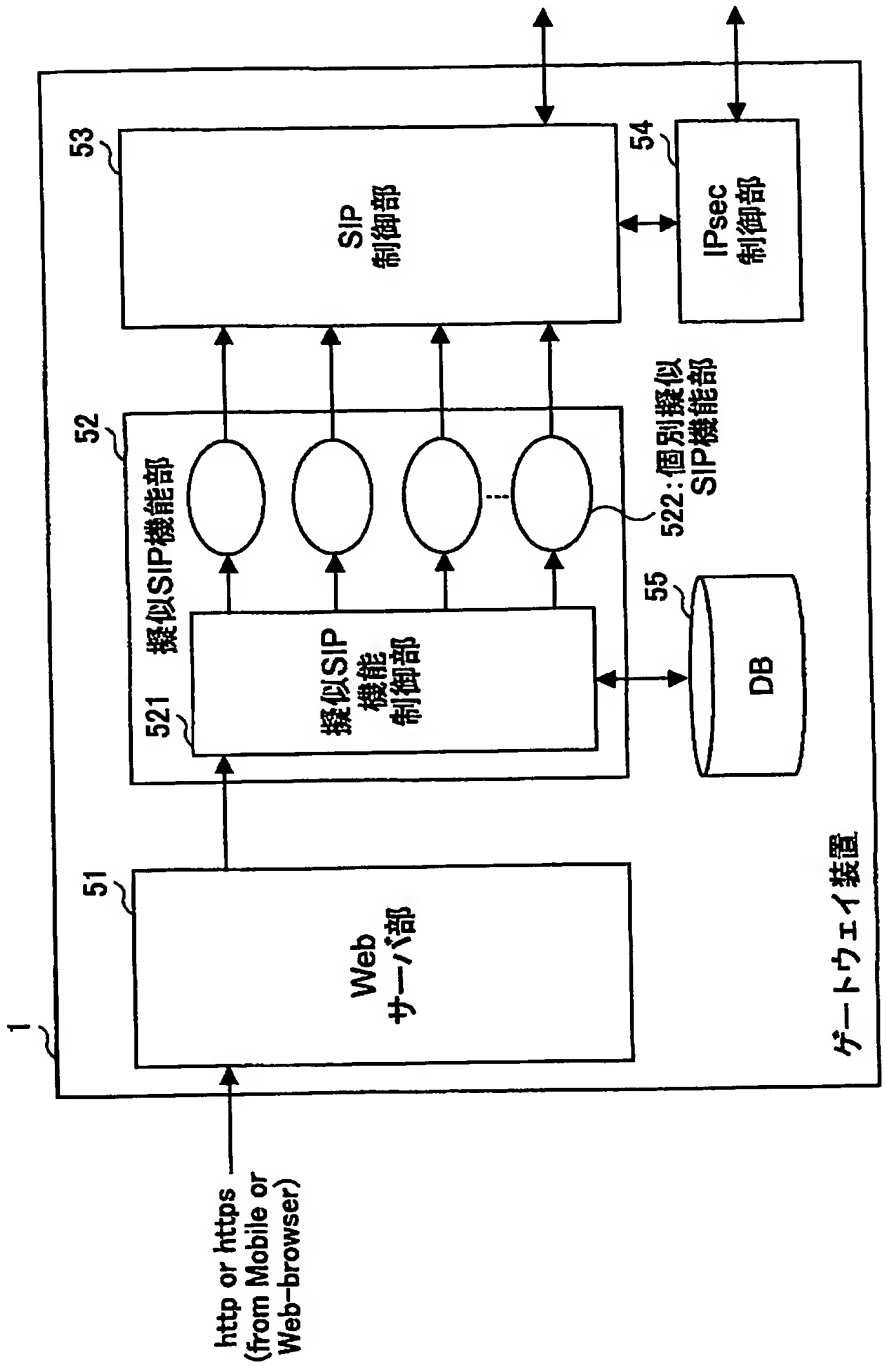
【図１３】

ユーザと接続先の対応を示すテーブル

ユーザ識別子	アクセス先の名前
×××　AAA,BBB,CCC,・・・・・	
⋮	⋮

【図１４】

ゲートウェイ装置1の機能ブロック図



【書類名】要約書
【要約】
【課題】　端末間でセキュアなデータチャネルを容易に構築するための技術を提供する。
【解決手段】　ネットワークに接続された第１の端末と第２の端末との間で暗号化通信チャネルを確立するための方法において、前記ネットワークに接続されたセッション管理装置と第１の端末との間で相互認証を行い、セッション管理装置と第１の端末との間で第１の暗号化通信チャネルを確立し、セッション管理装置と第２の端末との間で相互認証を行い、セッション管理装置と第２の端末との間で第２の暗号化通信チャネルを確立し、第１の暗号化通信チャネルと第２の暗号化通信チャネルとを介して第１の端末と第２の端末との間で鍵情報を交換する。
【選択図】　図１

特願２００４－０３４１７２

出願人履歴情報

識別番号　［３９９０３５７６６］

１．変更年月日　１９９９年　６月　９日
［変更理由］　新規登録
住　所　東京都千代田区内幸町一丁目１番６号
氏　名　エヌ・ティ・ティ・コミュニケーションズ株式会社